Utilising Journey Mapping and Crime Scripting to Combat Cyber Crime

Tiia Somer, Tallinn University of Technology, tiia.somer@ttu.ee
Bil Hallaq, University of Warwick, bh@warwick.ac.uk
Tim Watson, University of Warwick, tw@warwick.ac.uk

Abstract

Modern societies are now reliant on digital communication and networks for conducting a wide array of tasks, ranging from simple acts such as browsing the web through to mission critical tasks such as the management of critical infrastructure and industrial controls. This reliance shows a growing emphasis on strategic importance of cyberspace (Sharma, 2010). While organisations and individuals are keenly exploiting the benefits of cyberspace, these same platforms have also opened new avenues for nefarious actors in the pursuit of their criminal activities to attack, disrupt, or steal from organisations and individuals. Criminal organisations and lone criminals worldwide have access to powerful, evolving capabilities which they use to identify and target their victims allowing for the perpetration of a wide variety of cyber crimes.

This paper discusses ways in which utilising methods from typically non-cyber disciplines – business and criminology – can successfully be applied to the cyber domain in order to help in the fight against and prevention of cyber crime. Through the provision of a visual representation, this paper clarifies how journey mapping and crime scripting can help in building an understanding of the steps criminals undertake during execution of a cyber crime. In essence, within our work we have deconstructed the lifecycle of a crime events and translated these into a visualisation map to show the full event process, highlighting key steps as well as positive and negative events. Such work is useful to several roles and organisation types as it can aid in their decision processes when undertaking steps in pursuit, prevention, preparation and protection.

Keywords

Cyber crime, criminal journey mapping, cyber crime scripting, E-CRIME Project

Introduction

It is an established fact that the internet has greatly affected the way societies and people operate. Worldwide internet usage has increased to more than 3.5 billion users at the beginning of 2014 (Internet Usage and World Population Statistics, 2014). In addition to people, internet connectivity today extends to digital devices, with more things connected to the Internet than people. Gartner predicts that the number of internet connected devices will reach 25 billion for 2020 (Gartner, 2014).

While organisations and individuals are quick to exploit the business and personal benefits of internet, they often give less consideration that cyberspace offers a plethora of benefits to those who wish to attack them. Hacker groups, criminal organisations and espionage units worldwide have access to powerful, evolving capabilities, which they use to identify and target their victims and commit cyber crimes.

This research was conducted as part of the Economic Impacts of Cybercrime (E-CRIME) project of the Seventh Framework Programme, funded by the European Union. The majority of this work has been conducted with the help of desktop research and insights from a group of experts; the conclusions drawn and statements made rely on the Deliverable 2.3. “Detailed appendixes on cyber crime inventory and networks in non-ICT sectors” of the E-CRIME project. The work was conducted by means of a review of the existing literature and an evaluation of the published approaches, as well as by conducting expert interviews. Sources of information included journals and conference proceedings in the fields of law, criminology and information systems, reports published by think-tanks and law enforcement agencies as well as scholarly textbooks.

Interviews of experts were also undertaken as a further means of data collection with the main consideration being: even though cyber crime has been researched extensively, the specific criminal "journeys" and stepping stones the cyber criminals take within crime cycles have not been subject to such research methods previously to the best of the authors knowledge based on publically available information. An interview guide was prepared, which provided an informal grouping of topics to be covered during the interview. Once completed the results of the interviews provided extra data and some interesting nuances. The authors prioritized the interview results, since the main focus was the provision and mapping of criminal journeys.

The expert groups of interviews for this paper consisted of law enforcement operating at regional, national and international levels, industry based cyber security experts as well as experts from academia. The aim was to reach a common conclusion, and not to research single activities at the micro levels. Different focus groups each had a specific expertise and points of view to the topic of the research – cyber crime – which with the method chosen allowed for analysis of the experiences and requirements of a wider audience.

Cyber crime

Cyber crime is increasing in both complexity and intensity, reflecting an increased level of sophistication. For the purposes of this work our focus on cyber crime includes different aspects and extensions of modern crime: from development and sale of attack tools, services to plan and execute attacks and culmination in the laundering of stolen or illegally obtained assets. Cyber criminals increasingly operate in the same manner as legitimate business networks with clearly established business objectives and trusted supply chains for services or products that require outsourcing or development. The cyber criminals know what they are looking for, what goals they want to achieve and how to achieve these goals – and they are willing to spend time to research and plan their actions (CISCO 2014).

Given the complex nature of cyber crime and in order to understand and take efficient measures against it, it is imperative to gain deep understanding of the mechanics of cyber crime, from preparation, or pre-crime stages, to exit strategies and monetization, including everything in between the two including the committing of the actual crime. For the purposes of this paper we have performed several journey mapping exercises to describe the events and experiences that cyber crime perpetrators go through during a crime, using crime scripting techniques as found in traditional "offline" criminology. The research focus of this work has been on the crime itself, not the underlying causes of crime or the law enforcement actions following the crime. This mapping will help facilitate identification and testing of effective countermeasures, as well as facilitate further work in identification of possibilities to deter criminals and manage risks deriving from the perpetration of cyber criminal activities.

Three phases are critical to the development of our journeys from the perspective of the criminal:

1. Preparation phase
    a. Decision to engage in criminal activity
    b. Choosing a victim
    c. Choosing a method
2. Execution phase
    a. Conducting the crime
3. Monetization/Reward phase
    a. Exit

Cyber crime can be seen as a process where resources are required and decisions are taken at different stages in the process. The preparation phase includes pre-attack actions including committing to the initial decision to undertake a crime, deciding on the worthiness of an attack, identifying potential victims, and conducting targeted reconnaissance, but also a choice of an attack method including use of own means and abilities, or taking the decision to outsource respective capabilities. The execution phase includes drawing an attack plan and executing the attack itself, including entering the target system and conducting criminal activities within such systems. It

also includes lateral movement and finding additional opportunities for criminal action. The monetization phase includes direct or indirect monetary gain for the cyber criminals(s) and exit strategy. It is important to note that throughout any one criminal journey, the perpetrator can loop back to an earlier step (if a chosen attack method fails, they need to find a new one, or they may 'accidentally' find unforeseen vulnerabilities to take advantage of), or they can repeat steps for example, defacing the same website multiple times, or they may just quit once they realise the efforts are not worth the results.

Various sources show the developments of cybercrime and related threat landscape globally. ~~According to t~~The United Nations Comprehensive Study on Cybercrime of 2013 states that , ~~-~~cybercrime globally shows a broad distribution across financially driven acts, computer-content related acts, but also attacks against the confidentiality, integrity and availability of data and computer systems (United Nations 2013) which is key to take into consideration in understanding cyber criminal journeys. The 2015 RSA outlook on the changing threat landscape of cybercrime states that~~,~~ the most important trend developing within the past few years, is the rapid advancement of cybercrime-as-a-service model. What this development means, is that more criminals can participate in the chain and that these criminal do not need to understand the complete chain of the crime nor how to conduct any specific part of it, for example spam, DDoS or phishing. Nor do they need to have the technical requirements in house to the conduct of the crime itself (RSA 2015). The ENISA Threat Landscape 2015 states that from cybercrime-as-a-service model, the most mature are botnet-related service models (ENISA 2015). ENISA also states that the most rapidly growing service is provision of ransomware-related services. These points clarify the importance of journey mapping and crime scripting in order to provide those combatting cyber crime with a clear understanding of the complete crime cycle, including the various aspects and actors which may take part at different phases of a cyber crime.

Journey mapping

Journey mapping is a methodological tool that has been traditionally used in business to map customer experience, as well as in criminology generally under the name of crime scripts. Journey mapping is also often used by strategy consultancies and public organisations to shape customer strategies and public service transformational programmes. In criminology, crime scripts have been used to deconstruct complex crimes into component parts even from a relatively small data set. Within this work we have used such methods from these typically non-cyber disciplines and shown that they can be successfully applied to the cyber domain.

Crime scripting

The 'map'-style of output has been adopted and applied within a number of different disciplines where it is often referred to as a *script*. A script is a predetermined set of actions that define a well-known situation in a particular context (Borrion, 2013), or more specifically "[a] script is simply a sequence of actions which make up an event" (Brayley, 2011). Scripts are related to the concept of schema, i.e. "abstract cognitive representations of organised prior knowledge, extracted from experiences with specific instances". When the sequence of events being scripted encapsulates the conduct of a criminal activity (as in the case of cyber crime), the output is commonly referred to as a crime script (Borrion, 2013). Initially developed in psychology, scripts are now used in different fields from artificial intelligence to consulting.

Scripts can be used to present different crimes, but are believed to be of particular use for new or complex crimes (Brayley, 2011). It has also been suggested that crime scripts can be used as an innovative way to gain a more detailed understanding of complex forms of crime in a review of organized crime-reduction strategies (Levi, 2004). As previously stated in this paper, cyber crime is a rapidly developing field with an evolving trend of the cybercrime-as-a-service model. This will bring more participants into the cyber crime journey or cycle, making it more complex to understand for those dedicated to prevention and fight against cyber crime.

Why can criminal journey maps be useful?

By schematically representing an anticipated sequence of actions, scripts are able to provide us with a cognitive representation of how we believe a sequence of events has occurred and will occur (Borrion, 2013), including for our purposes, the steps a criminal takes to commit a cyber crime. In this situation, the value of crime scripting as a crime analysis mechanism is believed to be in its potential to assist in the fight against such crime (Borrion, 2013) through the identification of *pinch points*. For example, by graphically presenting the typical sequence of events for a crime that has been derived from many examples of that type of crime, analysts are able to identify specific metaphorical gates the criminal must pass through if their crimes are to succeed. Once these points are identified, the logic is that those seeking to prevent such crimes will now know where best to focus their energies, whether this be through legislative or regulatory changes, the development of new technological countermeasures, development of general awareness campaigns, the behaviour change of potential victims, or increased monitoring by police forces so as to capture or deter the cyber criminals. As stated in many cybercrime related sources, cyber crimes are becoming more complex, involving more parties each conducting independent steps within various phases of any one crime (RSA 2015, ENISA 2015)~~,~~. ~~the~~ The understanding of each step, however minor within this crime cycle, will become more vital. The journey maps developed provide a cognitive representation of how we believe a cyber crime takes place from preparation to monetization and exit.

Some crime scripts list a sequence of actions and don't draw a diagram, others draw a graphical representation showing a series of actions and decision points. In graphical presentations, scripts are usually drawn as series of boxes, linked by arrows indicating direction of flow (where boxes indicate actions or decisions). As the same crime can be committed in different ways, so can different routes/tracks co-exist on one script.

There are various levels of scripts and selection depends on the script's intended application (Brayley, 2011). For the purposes of the current work, we developed a high-level journey map detailing a general cyber crime cycle (Figure 1). This is a general depiction of a single cyber crime act, from which more detailed maps in different categories can been drawn. In order to be of practical use in understanding cyber crime, more detailed journey maps for different criminal journeys are needed, providing crime sequences from preparation to exit for these specific journeys.

Since there are no standard journey mapping rules or specific software for crime scripting (Brayley, 2011), we have used our own symbols and drawings. We grouped similar actions under broad terms: preparation, execution, and monetization. The journey maps developed provide a step-by-step high-level account of actions taken by the criminals throughout the crime. Crimes are a process which involves several steps leading to reaching an end-goal as identified by respective criminals. For example, the preparation phase includes various pre-attack actions, i.e. initial decision, deciding the worthiness of an attack, identifying victims, and conducting targeted reconnaissance. The preparation phase also includes the choice of an attack method, including the cyber criminal(s) undertaking an analysis of their own means and abilities and making the decision of outsourcing or buying solutions from external sources in case there is a resource or skills gap. The execution phase includes creating an attack plan and executing the attack, which comprises of entering or interfacing with target system and the actual criminal activities (i.e. distributed denial of service (DDoS), extortion, espionage, etc.) themselves. However, it is important to note that the tactics used by criminals do not always follow the above formalised decision points, meaning that in some instances decisions are made very quickly without conducting a full-scale analysis or creating a set of actual attack plans. A further important point to note, is that the criminal can loop back to any earlier phase as required by circumstances and in some instances they may choose to abort the undertaking for example in cases where the criminals might determine it is no longer cost-effective or the potential risk of getting caught is not worth the reward. The monetization phase includes a tangible payment in some form with laundering and/or mules often being utilised, although in some instances the criminals will not have a monetary objective which is discussed in the next section. The final result culminates in a personal gain or fulfilment of end-results as set out in the initial stages for the criminal(s).

Mapping and scripting a general cyber crime journey

Figure 1 represents a high-level journey map detailing a general crime cycle from the criminal's perspective. This general cyber criminal journey and journeys for any follow-on specific crimes have been developed with the help of desktop research and insights from experts as part of the E-Crime 7th framework project as already mentioned in this paper. The benefits for investigators of producing this visual representation of the general cycle are that;

(a) By identifying the commonalities in the conduct of what may seem very different cyber crimes, we can expose the sequence of events that underpin the majority of these.

(b) By comparing detailed maps of multiple different cyber crimes against this general crime cycle, those tasked with preventing and/ or defending against such crimes can see best where to focus their resources for maximum effect.

c) Experiment via virtualised or desktop exercises the application of countermeasures at various points along the pathway with the goal of taking forward the most effective ones for application in real word scenarios.

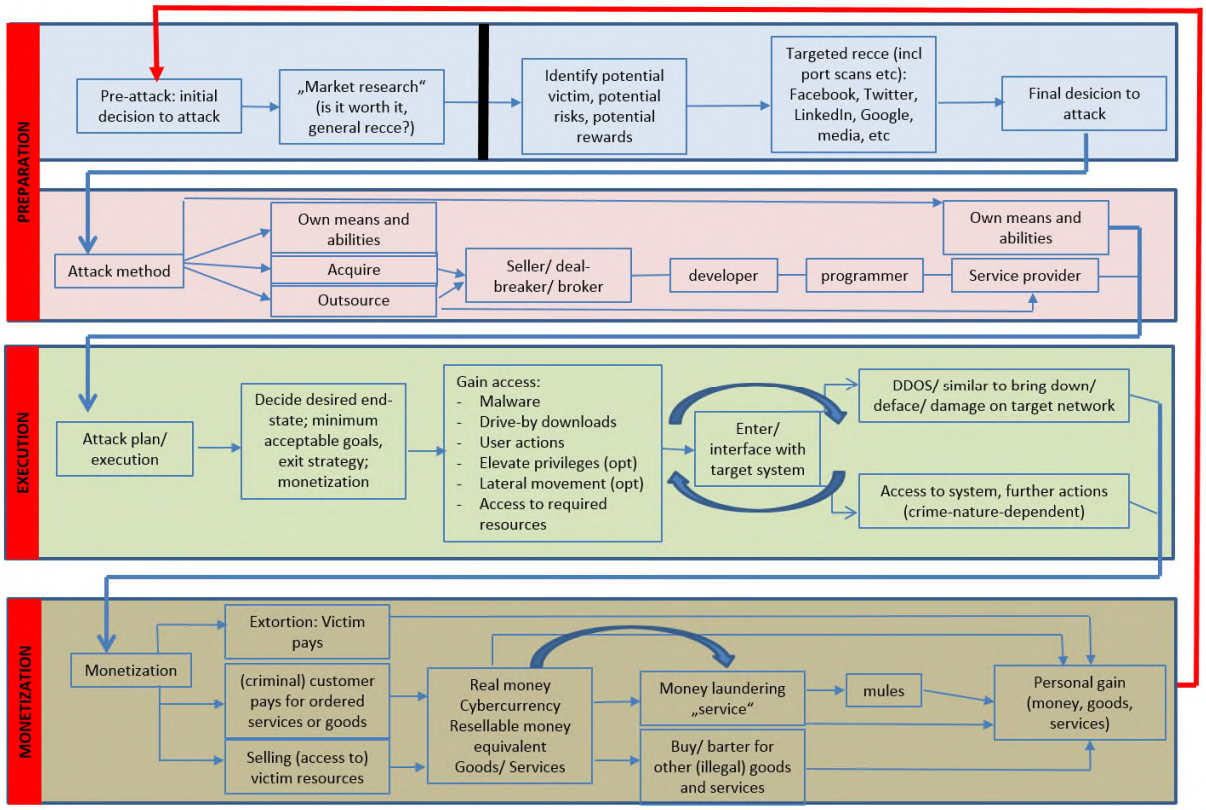

Figure 1: General cyber crime journey map

The preparation phase has two main components. Firstly the criminals need to decide whether or not to conduct the crime in the first place. This may be simply an opportunistic decision or it may include "market research" of some kind, in the sense of determining and weighing the costs and benefits of their options. The second component requires the identification of potential victims and attack methods, the conducting of targeted reconnaissance and finally deciding to execute the criminal act. The attack itself can then be executed in three ways, either; (1) by using their own existing means and abilities. As an example in case they have access to their own botnet, malware or exploit already, they will use these and will not go through all the steps in the process but move to the execution phase directly. (2) By buying the respective means and/or capabilities from other criminals – this brings other sectors into the process (special markets, forums, stores, sellers, brokers, developers, etc.), or (3) Outsourcing the required criminal activities by paying another criminal to conduct it as a service (crime-as-a-service).

The execution phase starts with an attack plan. In the plan the criminal decides upon a desired end-state, their minimum acceptable goals, and monetisation and exit strategies. During the attack, the criminal gains access to victim's resources through any number of means, including malware, drive-by downloads, user actions via phishing techniques or other illicit activities. Once the criminal gains access to the victim's system, they will map the compromised network, often looking for further opportunities to exploit. Thereafter the criminal enters or interfaces with the target system and based on their desired and decided goals and end-states they take the commensurate actions. Within this phase of mapping the compromised network, the criminal may notice other vulnerabilities that may become useful in their reaching of stated end-results and will take advantage of these, i.e. committing different crimes which were not originally part of their attack plan.

The monetization phase involves obtaining tangible benefits. These benefits include direct monetary gain, for example where the victim's monetary assets are stolen, or the victim pays the criminal directly in cases of extortion, such as ransomware or DDoS extortion schemes. Or indirect monetary gain whereby the victim's resources can be turned to tangible assets which are traded or sold, for example selling access to the victim's machine to others. The payment can be conducted in real currency, crypto-currency, resalable money equivalents (such as gaming assets), or in goods and services (real or virtual, legal or illegal). In some cases money laundering services are used, in other cases other means such as setting up mules to withdraw cash from banks might be used. Clearly though in some cases the monetization phase is excluded, examples of such cases include Hacktivists or those with ideological or other motivations.

In any case the crime ends with an exit strategy as set out by the criminal culminating in some type of personal gratification be it monetary or otherwise.

Conclusion

Within this report, the authors have shown how traditional crime scripting can provide useful insights into understanding the lifecycle of a general cyber-criminal journey. It also shows how methods and techniques from typically non-cyber disciplines can be successfully applied to the cyber domain. Such mapping and scripting can be modified and further detailed for specific crime scenarios and graphically represented. By graphically presenting the sequence of events constituting a cyber crime, risk management teams, forensic analysts, incident response teams and law enforcement agencies will be able to identify the specific stepping stones and pinch points that cyber criminals pass through in committing their crimes. Such work can help to facilitate the identification and testing of effective countermeasures including mitigation at scale, early prevention and the development of proportional disruption techniques.

References

Brayley, H., Cockbain, E., Laycock, G., 2011. The value of crime scripting: Deconstructing Internal Child Sex Trafficking, Policing, Volume 5, Number 2, pp. 132–143

Borrion, H., 2013. Quality assurance in crime scripting, Crime Science 2013, 2:6. Available online at: http://www.crimesciencejournal.com/content/2/1/6

CISCO, 2014. Annual Security Report. Available online at: http://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf

The Economic Impacts of Cyber Crime, FP7-SEC-2013.2.5-2. D2.3 Detailed appendixes on cyber crime inventory and networks in non-ICT sectors. T.Sõmer, R.Ottis, T.Lepik, M.Lagazio, B.Hallaq, D.Simms, T.Mitchener-Nissen. March 2015

ENISA Threat Landscape 2015. ENISA 2015. Available for download at: https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape/etl2015

Gartner, 2014. http://www.gartner.com/newsroom/id/2905717

Internet Usage and World Population Statistics, 2015. http://www.internetworldstats.com/stats.htm

RSA 2015. CYBERCRIME 2015: An Inside Look at the Changing Threat Landscape. Available online at: https://www.emc.com/collateral/white-paper/rsa-white-paper-cybercrime-trends-2015.pdf

Sharma, Amit, "Cyber Wars: A Paradigm Shift from Means to Ends", Strategic Analysis, Vol. 34, No. 1, 2010, pp. 62-73. http://www.tandfonline.com/toc/rsan20/34/1

United Nations 2013. United Nations Office on Drugs and Crime, Comprehensive Study on Cybercrime, February 2013. Available online at: <http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf